REMARKS

Reconsideration and further examination is respectfully requested.

The Examiner is thanked for the careful consideration of Applicants' previous remarks, and the additional description of the Examiner's analysis. Applicants believe that the below remarks support the Applicants' continued belief in the novelty of the claims in view of Mittra. Upon review of Applicants' remarks, if the Examiner does not support Applicants' position, Applicants' request an interview with the Examiner to discuss remaining points of contention, to facilitate issuance of this application.

Rejections under 35 U.S.C. §102

Claims 1-152 were rejected under 35 U.S.C. §102(b) as being anticipated by Mittra, U.S. Patent 5,748,736.

It is noted that in order to support a rejection under 35 U.S.C. §102, *every* limitation in the claim must be found or suggested in the prior art. Mittra does not teach every limitation of the claim, and thus cannot be used to support a rejection under 35 U.S.C. §102.

Claim 1 recites "...A communication system comprising ... a plurality of multicast devices forming a shared multicast distribution tree... a host device ... a key server... and a designated device, separate from the key server, through which the host device requests access to the shared tree associated with a group..."

Mittra does not have "a designated device separate from the key server through which the host device requests access to the shared tree..." Rather, Mittra describes at column 7, lines 45-65:

"...Joining a secure multicast group requires the joining member first to set up a separate secure channel with the GSC of the group (using a unicast communication line). The purpose of the secure channel is to facilitate and isolate confidential communication between the GSC and this member during the time that the member is part of the group... Upon receiving a join request (and approving it), the GSC inserts the member's identification and information concerning the secure channel in a private database it maintains. In this way the GSC has full knowledge of the group membership and can communicate with each member separately and securely when required. The member must also store information concerning the secure channel for future communication with the GSC... All communications from the GSC must include a message digest and be digitally signed so that receivers may verify that the message has not been corrupted and the sender was actually the GSC... Only the GSC maintains information concerning group membership; members do not know about each other (except that receivers may need to know the list of authorized senders)..." ..."

Mittra also states, at column 8, lines 14-22:

"...Once the GSC and the new member have authenticated each other and have agreed on a secret the GSC needs to provide the new member with information that will allow it to encrypt and/or decrypt the multicast transmission. At this point the GSC also needs to change the group key (Kgrp) which provides access to the multicast transmissions. This is done to prevent the joining member from decrypting previous transmissions to which it should not have access..."

Thus, in Mittra, when a device seeks to join a group:

1). The host establishes a separate side channel communication with the GSC.
2). Within the channel, the host issues a 'join request' to the GSC start authentication. In response to the 'join' request, the GSC starts the authentication process
3). When authenticated, the host receives a group key from the GSC
4). The host communicates within the group.

Mittra does not describe "...and a designated device, *separate from the key server,* through which the host device requests access to the shared tree associated with a group..."

Because Mittra does not describe a designated device separate from the key server, it cannot be used to reject claim 1.

The Examiner states, at pages 16-17 of the Office action received August 9th, 2005:

"... The examiner would like to point out that the amended claim states: "a designated device, separate from the key server, through which the host device requests access to the shared tree associated with a group..." Hence, there lies a device of some type (possibly a gateway or router) that the host uses to access the tree. The use of a gateway or a router or any number of devices to enable a host to access another device(s) is inherent and well known in the art. Plus, if the "designated device" were not a router or a gateway, the claimed "designated device" still does not performing any novel task nor is it performing a task that could not be performed if it were implemented into the host or key servers. For these reasons, the examiner must stand by his rejections..."

The Applicants would like to make the following points:

With regard to the Examiner's statement that "The use of a gateway or router or any number of devices to enable a host to access another device(s) is inherent and well known in the art. Plus if the "designated device" were not a router or a gateway..."

Applicants would like to emphasize that in no point in the specification or any patent office correspondence have the Applicants stated or implied that the designate device is not a router or a gateway. And note that the term Designated Router (DR) is used throughout Applicants' specification.

With regard to the Examiner's statement that the claimed "designate device" still does not perform any novel task nor is it performing a task that could not be performed if it were implemented into the host or key servers..." Applicants respectfully submit that such an argument ignores the language of the claim, which states that the devices are *separate*, and rather

seems to draw an equivalency argument, which is not an appropriate argument in support of a rejection under 35 U.S.C. §102.

Applicants respectfully disagree submits that the Examiner is not affording patentable weight to the limitation of 'separate from the key server,' this separation being one of the enabling features that allows the present invention to have a distinct advantage over the different architecture described by Mittra.

In reading the Examiner's statements, it appears that the Examiner's argument against the claims being novel is that Mittra teaches both items, and they could both be the same (i.e., this is how Applicants interpret the statement "the claimed "designated device" still is not performing any novel task nor is it performing a task that could not be performed if it were implemented into the key servers..."

Applicants disagree, and submit that there is a fundamental difference between having the two functions integrated in one server, and the functions separate, as in the claimed invention. This difference provides a distinct advantage in protecting the system from attack by a flurry of Join requests; if Join requests and authentication are tied together, as in Mittra, the system can become flooded. Applicants described such a situation at pages 2-3 of the Background section of Applicants' specification, which describes:

> "... Another attempt to protect the shared tree involves the authentication of control messages between multicast routers. Specifically, the multicast routers exchange various control messages for, among other things, joining the shared tree. These control messages are authenticated hop-by-hop according to a predetermined authentication scheme. By authenticating all control messages, only authorized multicast routers are able to join the shared tree... Unfortunately, neither data encryption nor control message authentication prevents an unauthorized host from joining the shared tree and thereby consuming valuable communication resources. Because authentication operates only between the multicast routers, an unauthorized host can still join the shared tree, specifically by sending a join request, for example, using IGMP or other group management mechanism. The multicast routers establish the appropriate

multicast routes for routing multicast packets to the unauthorized host, perhaps even using authentication to perform hop-by-hop authentication. As a member of the shared tree, the unauthorized host receives multicast packets. This is true even if the multicast packets are protected using data encryption, in which case the unauthorized host simply discards the encrypted multicast data..."

In contrast, the present invention enables "An authenticated host is added to the shared tree, while a host that cannot be authenticated is prevented from joining the tree..."

It would appear that the Examiner has not appreciated the patentable weight of the limitations of the claims. However, it should be appreciated that the present invention, by permitting a method to separately authenticate a host's join requests overcomes a problem that is not capable of being overcome by Mittra; namely, join requests from unauthorized hosts will *not* be forwarded up the multicast tree for authentication processing. Mittra provides no such protection.

Thus there are several elements of claim 1 which are not recited in Mittra. In particular, Mittra neither describes nor suggests "a designated device, separate from the key server, through which the host device requests access to the shared tree associated with a group..." Rather Mittra provides authentication and key distribution from a *single* device. In addition, Mittra neither describes not suggest "...the host device obtains access information from the key server for the host device to request access to the shared tree associated with the group, the access information including authentication information unique to the host device/group pair ..." Rather, while Mittra does state that a side channel is established with the host device, no mention is made that authentication information used in the side channel is 'unique to the host device/group pair...'

Accordingly, for at least the reason that every limitation of claim 1 is neither described nor suggested in Mittra, the rejection under 35 U.S.C. §102 should be withdrawn. Independent claims 16, 28, 40, 61, 68, 75, 87, 99 and 122 have been amended to include limitations similar to those of claim 1 which assist to distinguish the claims over Mittra, and thus the rejection under 35 U.S.C. §102 for these claims should be withdrawn as well. Dependent claims 2-15, 17-27, 29-39, 41-60, 69-74, 76-86, 88-98, 100-121 and 122-144 serve to add further patentable limitations to their parent independent claims, but are allowable for at least the reason put forth above with regard to their parent independent claim.

Conclusion

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Lindsay G. McGuinness, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

11/7/05
Date

Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
Steubing McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-147
Dd: 11/09/2005